第4章 Luaスクリプトでフィールドやパケット解析関数を定義する

ダイセクタを自作して独自プロトコルの解析にトライ

竹下 恵

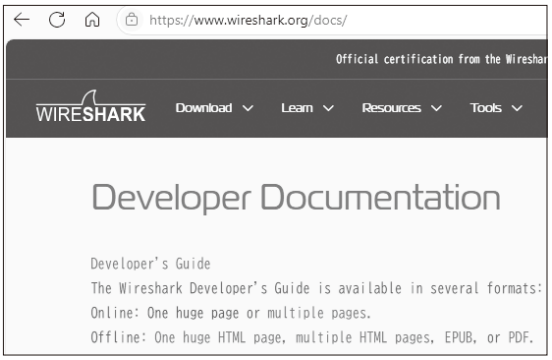

図1　ダイセクタのAPIの詳細はWiresharkのDeveloper Guideが参考になる
具体的にはWireshark's Lua API Reference Manualのセクションに記載がある.
https://www.wireshark.org/docs/

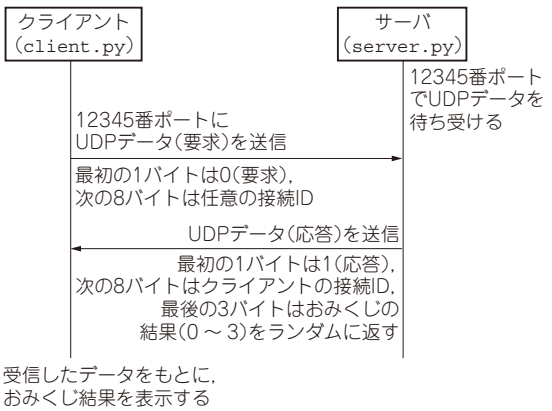

図2　独自プロトコル題材「おみくじアプリケーション」の通信の流れと処理内容

プロトコルを定義するダイセクタは自作できる

● 独自プロトコルの解析にもWiresharkを使える

Wiresharkは現在，3000以上のプロトコル，26万5000以上の実フィールド，生成フィールドを持ちます．標準化された通信であれば，通常のパケット・キャプチャで解析できないパケットはまずありません．しかも，Wiresharkは自分でダイセクタ(Dissector)と呼ばれるプロトコルの定義を作成したり，ポスト・ダイセクタ(Post Dissector)を用いて既存のダイセクタを拡張したりできます．

例えば，自社の組み込み製品で用いる独自の通信の手続きであっても，Wiresharkのダイセクタを定義することで，Wiresharkの充実したGUIやグラフなどの機能を使ったデバッグやトラブルシューティングが行えるようになります．

● 自作するならLuaスクリプトがおすすめ

Wiresharkのダイセクタは，WSGD(Wireshark Generic Dissector)と呼ばれるテキスト・ファイルや，Lua言語，C言語で開発できます．WSGDはコンパイルが不要ですが，複雑な処理を記述することが困難です．C言語はコードが非常に長くなり，Wiresharkのコードとマージしてコンパイルする手間もかかります．そこで，一般的にはスクリプト言語のLuaがダイセクタに利用されます．

LuaスクリプトによるWiresharkのダイセクタのAPIの詳細は，Wiresharkの開発者ガイド(**図1**)のWireshark's Lua API Reference Manualのセクションが参考になります．

・Wiresharkの開発者ガイド
https://www.wireshark.org/docs/

本章でやること…ダイセクタを自作して独自プロトコル解析に挑戦

● 独自プロトコル題材…おみくじアプリケーション

簡単なダイセクタを自作して独自プロトコルの解析にチャレンジします．ここでは，簡単なおみくじのクライアント・サーバ型アプリケーションを考えてみます(**図2**)．本章で作成するプログラム類は次のウェブ・ページよりダウンロードできます．

https://www.cqpub.co.jp/interface/download/contents2025.htm